



XIOX CORPORATION

DO NOT FILE COPY ORIGINAL

January 4, 1994

RECEIVED

JAN 13 1994

FCC MAIL ROOM

Office of the Secretary
Federal Communications Commission
Washington, DC 20554

RE: "CC Docket 93-292"

Dear Commissioners:

Regarding your December 2 release on Toll Fraud, Xiox would like to comment on four of the rulemaking proposals. As the developer of the first anti-hacker product line to be warranted against hacking (underwritten by the Travelers for up to \$100,000 per year), Fort Knox™, we feel uniquely qualified to comment on: (1) achieving closer coordination between the industry, consumers, vendors, law enforcement agencies, Congress, and the Commission to aid in the detection and prevention of toll fraud; (2) improving consumer education initiatives by the Commission, consumer groups, and the telecommunications industry; and (3) the determination of whether tariff liability provisions fail to recognize an obligation by the carrier to warn customers of toll fraud risks of using carrier services are unreasonable.

Since the technology employed by Xiox in protecting the consumer from toll fraud is extensible into the network, we would like to add a final comment on: (6) measures to prevent cellular and Line Information Database (LIDB) fraud.

CLOSER COORDINATION

Regarding the closer coordination between all effected parties, Xiox would like to draw your attention to: (a) the apparent end-user environment dichotomy between being open and being secure, (b) our experience in the sequence of responses by consumers to an event of toll fraud, (c) the current, latent, industry capability to bring artificial intelligence protection against toll fraud, (d) the acceleration of telecommuting fueled by The Federal Clean Air Act and the National Information Infrastructure (NII) vs. toll fraud.

No. of Copies rec'd 028
List A B C D E

CONSUMER EDUCATION

Regarding the improving of consumer education, Xiox would like to draw your attention to the need for artificial intelligence to make a realtime distinction between users and hackers.

TARIFF CHANGES

Regarding the determination on the reasonableness of current tariff liability provisions to warn customers of toll fraud risks, Xiox would like to draw your attention to: (a) the existence of the combination of technology and financial protection that would make certain users less risky, and therefore, less costly to serve; (b) the currently available option to carriers to offer usage warranted against toll fraud, the flip-side of users making themselves less costly to serve; (c) the need to include hierarchical security thresholds, alarming of user administrators wherever they may be at the time of hacking attack, the capability for user administrators to affect the hacking situation as it occurs, and a fail-safe mechanism to back-up user administrators in a secure user environment; and (d) the ineffectiveness of carrier trunk screening as a toll fraud prevention mechanism.

PREVENTION OF LIDB FRAUD

Regarding the measures to prevent Line Information Database (LIDB) fraud, Xiox would like to draw your attention to extending consumer level technology into the network.

OPEN vs. SECURE

Closer coordination between all effected parties should be directed towards solving the dichotomy between being open and being secure. Xiox' experience in providing toll fraud protection indicates the majority of consumers who are victimized by toll fraud choose to become more secure by becoming less open. As the Notice of Proposed Rulemaking (NPRM) indicates in paragraph # 5, "(The) new telecommunications technologies that offer the most convenience and flexibility for users, are often also most likely to present new toll fraud opportunities." As a result, users avoid these new technologies. In fact, the vast majority of users have also disconnected or disabled at least one older, previously-in-use technology as a result of toll fraud, or the threat of toll fraud.

Instead of finding solutions that don't hinder the use of new technologies, and ensuring that telecommunications equipment and services remain accessible; users are instructed by the industry (both equipment vendors and carriers) as to which existing and new features should be turned off, disconnected, and disabled; and in which order. Instead of finding solutions that don't hinder the use of new technologies, and ensuring that telecommunications equipment and services remain accessible; manufacturers now present the absolute lack of a previously available technology as a new toll fraud prevention feature.

The industry response to the point raised in paragraph #16, "(The) new technology of multiple node virtual networks using many PBXs and other sophisticated network terminating equipment...(making) the impact of fraud more serious;" is often to turn off the new technology in favor of network based security inherent in calling cards. Unfortunately, for users the network based solution may be more expensive, offer less accountability, and be less controllable.

Xiox' experience in providing toll fraud solutions is that the above scenario, of being less open in order to be secure, is not the only user option. The above scenario, of being less open in order to be secure, is not the best user option. The above scenario, of being less open in order to be secure, is ultimately not what is best for all effected parties.

Technology exists today using Artificial Intelligence (AI) and Voice Password Analysis (VPA) that is so resilient to toll fraud attack, it is possible to be both open and secure. Technology to prevent toll fraud exists today that is so resilient to toll fraud, both current and new applications can be used and still be secure. Technology exists today that is so resilient to toll fraud attack, insurers are willing and able to underwrite \$100,000 toll fraud warranties. Therefore, Xiox urges the Commissioners to include the integration of such technology by the CPE-owner in the, "Definition of specific responsibilities," called for in paragraph #25.

CONSUMER RESPONSES TO TOLL FRAUD

Closer coordination between all effected parties should also be used to help the consumer move through the normal stages of dealing with toll fraud, prior to problem resolution. Xiox' experience in providing toll fraud protection indicates consumers (after education, but prior to their first toll fraud incident) often function as if toll fraud is something awful that happens to others. Even after the frequency of incidents increased from 1 out of every 18 PBXs in 1992, to 1 out of every 6 PBXs in 1993 (source Telecommunications Advisors, Inc.), users still functioned under the assumption that untested environments were safe by sole virtue of not yet being victimized.

In Xiox' experience, the next stage of consumer behavior is to disconnect and disable existing technology in hopes of locking hackers out of their environment. This second stage is as naive as the first stage. Plus, in addition to locking out some hackers, the consumer also locks out their users.

The final response the consumers go through occurs after a second toll fraud incident. Consumers then seek, "...to find solutions to each fraud problem without hindering the use of...new technologies," as called for in paragraph #5. Xiox urges the Commissioners to advocate all effected parties (consumers, manufacturers, carriers, etc.) move to the final response quickly, and move to this response through the incorporation of anti-hacking technology.

USING AI TO STOP TOLL FRAUD

Closer coordination between all effected parties should be used to bring existing AI to bear on the toll fraud problem. The prevention and quick reaction to fraud by users provided by carriers called for in paragraph #16, and "(The) prompt remedial action [detect and remedy in (a) timely manner]," in paragraph #17, require either constant vigilance of experts, or the use of technology that can imitate the behavior of those experts.

Such AI technology would need to learn legitimate user behavior in order to distinguish that behavior from hacking. In addition, such AI technology would need to simultaneously consider the relative weight of multiple factors of learned user calling behavior in order to distinguish legitimate users from hackers. The AI terms for this type of technology are heuristics (self learning) and fuzzy logic (eyeballing a situation).

Products with both heuristic and fuzzy logic AI will respond to a potential toll fraud incident infinitely quicker than the preset parameters called for by SIA in paragraph #18. And products with both heuristic and fuzzy logic AI are easily modified to be internal to telecommunications equipment as proposed by Western in paragraph #19. Xiox urges the Commissioners to consider the lessening effect on total toll fraud to be allocated between IXC's and customers, if such AI technology were used.

TELECOMMUTING AND TOLL FRAUD

Closer coordination between all effected parties is needed more today than any previous time, due to the sociological trend of telecommuting. According to the December 14, 1993 Wall Street Journal, telecommuting increased by 15% in 1992 to 7.6 million workers. Adding to that 15% growth rate will be the pressure of the Federal Clean Air Act requirements for rising minimum percentages of employees telecommuting and/or car pooling by the year 2000, and the capability of companies to support telecommuting increasing with the available technology in the NII.

Companies with telecommuting employees often want their telecommuting employees to use the company's on-network lower cost usage, want their telecommuting employees to call through the company phone system in order to be able to track and manage activity, and want their telecommuting employees to use the advanced voice technology located at the company site as if they were on-site.

All of these desires require the use of the remote access technology referenced by ARINC in paragraph #17. Xiox has observed that companies that deinstalled, disconnected, or disabled remote access in response to toll fraud, are now turning back on that same technology under the name telecommuting.

All of the remote technology can be secure with the use of the right anti-hacking technology. For example, telecommuting and remote access are two of the applications Xiox' \$100,000 warranty will cover.

Xiox urges the Commissioners to add telecommuting to the impetus behind the rulemaking, to consider telecommuting in making any new rules, and to include telecommunications security technology in those rules.

EDUCATION ON TECHNOLOGY

In Xiox' opinion, consumer education on toll fraud should be at least equal to, if not greater than, the education available to the hacker community. Between magazines, telemarketing of hacking education materials, and bulletin boards; the information available to hackers on available technology to use in hacking is alarmingly extensive.

Xiox urges the Commissioners to facilitate the inclusion of available anti-hacking technology in any and all education on toll fraud, such as that discussed in paragraphs #13 and #26.

DISCOUNTED LD FOR LESS RISKY CUSTOMERS

Strengthening tariff liability provisions warning customers of toll fraud risks, is just one of the, "...specific ways to achieve closer and continuing coordination among the institutions fighting toll fraud," as requested in paragraph #13. Xiox suggests that another way to achieve the coordination is to mandate carriers provide incentive to consumers to reduce toll fraud risk.

In paragraph #18, SIA proposes that the Commission find customers responsible for toll fraud, "...if they fail(ed) to obtain monitoring services or obtain them and fail to act upon (them)." If this were to become true, then customers who volunteer to assume that risk (by employing warranted toll fraud prevention equipment) should be rewarded.

In paragraph #22, Allnet contends, "...that if IXC's are required to insure end users against theft, then IXC's should be permitted to refuse to serve high risk end users." If this were to become true, then customers who volunteer to assume that risk (by employing warranted toll fraud prevention equipment) should be financially encouraged by the IXC's.

Xiox urges the Commissioners to mandate to the carriers the proactive step of discounting long distance to those users who mitigate the IXC's risk by assuming responsibility upfront through employment of warranted toll fraud prevention equipment. Xiox' contention is discounted long distance to customers who meet a tighter/higher definition of responsibility is ultimately less costly for all concerned than the alternatives of liability determination, mediation, or arbitration that are discussed in paragraph #25. And Xiox contends discounted long distance for customers with warranted toll fraud equipment could eliminate any burden on residential ratepayers as discussed in paragraph #25.

In paragraph #16, most commenters, "...concur...that the Commission (should) require IXCs to offer, at cost-based rates, services designed to help users prevent, and react quickly to fraud." In paragraph #18, SIA proposes, "...that the Commission require IXCs to offer, at cost-based rates, services designed to help large users react quickly to toll fraud..." Xiox is proud of its business association with MCI, who (through their MCI Detect Program) does in fact provide Xiox Fort Knox™ warranted toll fraud prevention equipment at their cost. However, Xiox contends that either discounted long distance for customers who employ warranted toll fraud equipment, a warranted long distance alternative from the carriers, or both are needed to achieve the closer coordination desired by the Commission in paragraph #13.

SECURE LONG DISTANCE

Xiox suggests that another way to achieve the coordination, among the institutions fighting toll fraud, as called for in paragraph #13 is for the Commission to mandate the carriers offer their users a secure usage alternative. With the proper technology and the insuring of risk based on that technology, carriers would be able to provide long distance service that is inherently safe to use for all advanced applications.

Xiox is apparently joined in this suggestion by the many commenters mentioned in paragraphs #16 and #18 and described above. The case for a secure LD offering is made very strongly by PE in paragraph #17, where PE, "...contends that a carrier should not be permitted to limit liability unless the carrier has installed the best available techniques to detect and prevent remote access toll fraud..."

As is the case with consumers receiving long distance discounts for using warranted toll fraud equipment, Xiox contends a secure LD alternative is ultimately less costly for all concerned than the alternatives of liability determination, mediation, or arbitration discussed in paragraph #25. And Xiox contends that a secure LD alternative could eliminate any burden on residential ratepayers as discussed in paragraph #25.

While Xiox would be forced to take the affirmative position in the Commission's paragraph #26 question, "In light of our tentative finding that tariff liability provisions that fail to recognize a duty by the carrier to warn customers of risks of using carrier service are unreasonable, we ask whether a failure to offer services to limit customers' exposure should be considered an unreasonable practice (?)," Xiox wants the Commissioners to be aware, one of our carrier business partners will be announcing a secure LD alternative for their customers this quarter.

REQUIREMENTS OF WARRANTED TOLL FRAUD EQUIPMENT

With either discounted LD or secure LD, the underlying warranted toll fraud equipment would need to include hierarchical security thresholds, alarming of user administrators wherever they may be at the time of hacking attack, the capability for user administrators

to affect the hacking situation as it occurs, and a fail-safe mechanism to back-up user administrators. The first two of four objectives expressed by ARINC in paragraph #17, "1) toll fraud prevention (carriers' detection and prevention plans); 2) prompt remedial action (detect and remedy in timely manner);" the quick reaction called for by SAI in paragraph #18; and the, "...automatic alarm algorithm that would page a PBX attendant who could shut down the PBX from a remote location," called for by Allnet in paragraph #22 are all accomplished by Xiox' Fort Knox™ product line. Xiox urges the Commissioners to include the requirements listed above in vendor and carrier, equipment and services.

CARRIER TRUNK SCREENING

The Xiox Fort Knox™ product line facilitates use of hierarchical security thresholds (including voice password analysis); intelligent alarming; immediate, remote administration of a hacking situation; and autokilling of user IDs, facilities, and technologies through AI monitoring of each user's activity. Monitoring only the aggregate usage on trunks, as suggested by SIA in paragraph #16, would not allow for discrete enough information. The effect of the mass volume would be to average out the pattern exceptions that point to hackers. Discount LD or secure LD both need CPE located monitoring of individual user calling patterns, as accomplished by the Xiox Fort Knox™ product line.

PREVENTION OF LIDB FRAUD

While monitoring trunk usage is not discrete enough to be usable, the Xiox Hacker Preventer™ technology could be extended to use the heuristic learning of LIDB pattern profiles; the fuzzy logic monitoring of the LIDB customer account usage pattern; the hierarchical security thresholds; intelligent alarming; and the autokill, fail-safe mechanism to prevent calling card fraud. Xiox is very interested in working with IXC's and LEC's to utilize our proprietary AI and voice password analysis in the network.

CONCLUSION

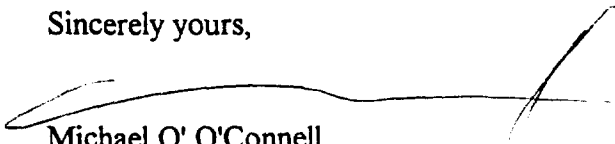
Paragraph #26 asks, "We also seek comment on whether there is software or equipment that customers should install in their CPE to prevent fraud." To this question, Xiox answers YES with all the conviction of our \$100,000 per Fort Knox™ installation toll fraud warranty. In response to the final request in the paragraph, for rule proposals; Xiox urges the Commissioners to:

- 1) define consumer responsibilities to include the installation of warranted toll fraud prevention equipment,
- 2) define vendor and carrier responsibilities to include providing toll fraud prevention through warranted toll fraud prevention equipment rather than disabling and disconnecting features and applications,
- 3) require AI utilization by all effected parties, to lower the total amount of toll fraud,

- 4) consider telecommuting in all rule making, including technology needed to make telecommuting secure,
- 5) require vendor and carrier education of the consumer include viable, warranted toll fraud equipment,
- 6) mandate carriers provide discounted LD to consumers using warranted toll fraud prevention equipment,
- 7) mandate carriers offer a secure LD alternative,
- 8) mandate prevention, prompt remedial action, and automated alarming in vendor and carrier, equipment and services,
- 9) mandate AI technology in LIDB use for calling card usage.

Xiox gratefully appreciates the opportunity to comment on the NPRM. Please call me with any questions, comments, and concerns.

Sincerely yours,



Michael O' O'Connell
Vice President of Marketing

cc: The Honorable Congressman Edward Markey
Gerard Waldron, Senior Counsel, Subcommittee on Telecommunications and Finance
John Haugh, Chairman, Telecommunications Advisors, Inc.
Frank Scheckton, Director, the Travelers
Curtis Weeks, Vice President, AT&T GBCS
Edward O'Malley, Vice President, MCI
Jim McGovern, Vice President, Norstan
Richard Faleti, Vice President, NTI
Robert Fox, Vice President, Sprint
William Welling, Chairman, Xiox



- ◆ Protection from telephone "hackers" attempting to access your telecomm environment.
- ◆ Realization of remote-access service cost-savings without the risk of fraudulent use.

XIOX FORT KNOX FAMILY™

Every telephone system can be compromised! Hackers can easily attack... 800 numbers, travelling executives, telecommuters, voice-mail, automated attendants, modem pools, electronic mail, teleconferencing bridges, ACD's, telephone system networks, and remote maintenance ports.

Toll-fraud costs U.S. businesses billions of dollars each year, eroding corporate profits and costing victim companies millions of dollars in lost personnel time, litigation, and problem resolution. In addition to these costs, the victims of toll-fraud risk the security of sensitive information conveyed either by telephone or on data networks.

The Xiox Fort Knox family of products provides comprehensive protection against toll-fraud and other illicit entry to the corporate telecomm network. The Xiox Fort Knox family of products, alone or in combination, act as an intelligent agent tracking and stopping fraudulent use.

- ◆ Secure access to remote maintenance ports, voice-mail systems, and modem pools.
- ◆ Automatically and in real time senses user profile deviations and terminates fraudulent use.
- ◆ Secure monitored access for customers, traveling employees and telecommuters.
- ◆ Protection against unauthorized electronic access to vital corporate information.
- ◆ Greater visibility through printed reports on Telecomm system access.



XIOX CORPORATION
Block Hacking with Force...

XIOX FORT KNOX FAMILY™ XHP: Hacker Preventer™ ♦ Hacker Deadbolt™ ♦ Hacker Tracker™

The members of the Fort Knox family (see chart) can help you block hacking in the following ways:

Blocking...	The XIOX system that will...	
	Track	Stop
Hackers who trip alarms accessing the system	XHP	XHP
Hackers who trip alarms leaving the system	XHP/ XHT	XHP
Hackers who don't trip alarms	XHP	XHP
Hackers who try to reconfigure the user's system	XHP/ XHDB	XHP/ XHDB

Xiox XHP - Hacker Preventer

Utilizing Artificial Intelligence to separate hackers from users, the Xiox Hacker Preventer (XHP) protects entire telecommunications systems, while still allowing full use of all of the systems' money saving features. XHP provides protection by:

Tracking Hackers

- Robust reporting capabilities include Authorized User, Call Detail, Active User I.D.'s and Daily Activity by User I.D.

Stopping Inbound Hackers

- 3 levels of access protection including user I.D. and password, verbal password(s), and alarming.

Stopping Outbound Hackers

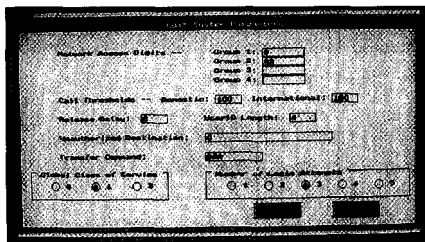
- User I.D.'s can be easily tied to specific destination or restricted from destinations, and PBX leaks are plugged automatically.

Stopping Hackers Who Don't Trip Alarms

- Proprietary user profiling, automated accumulation of profiles, and artificial intelligence comparisons to profiles separates hackers from users.

Stopping Hackers Who Try to Change Systems

- User configurable mixtures of spatial security, single-use with alarming, and automated connection with AI monitoring protect sensitive destinations such as remote ports of voice-mail and PBXs.



Configuration and maintenance can be accomplished either by secure telephone or using the DOS-based configuration utility provided with the XHP.

Xiox XHT - Hacker Tracker

The Xiox Hacker Tracker (XHT) is a cost-effective, dedicated software package that reports on PBX traffic through the use of Station Message Detail Recording (SMDR) data shared with any call accounting system. The XHT comes pre-configured with the most useful reports for tracking and trapping illicit users. The XHT includes complete, easy-to-follow software documentation, and

allows you to silently monitor system usage and traffic to high-fraud destinations such as the 809 area code and foreign countries. Features of the Xiox Hacker Tracker provides protection by:

Tracking Outbound Hackers

- Informative reports configured for immediate use including garbage records hiding hackers, traffic to high-fraud areas, voice-mail activity, activity by trunk, and incoming calls.
- Ability to create custom reports to monitor potentially vulnerable points of customer networks.
- Dialing-pattern recognition templates allow for setting of traps/alarms for specific hacking attacks.

Xiox Hacker Tracker Technical Requirements:

- Requires IBM PC-AT, PS/2 or compatible 80386 or 80486 based computer with minimum 585kB available RAM, 25 MB available hard-disk storage per 100,000 calls stored, 3.5" 1.44MB floppy drive, video monitor (EGA, CGA, or VGA), parallel printer port, parallel printer, two RS-232 serial ports, and DOS version 3.1 or higher. Also requires delivery of SMDR from customer PBX or key system via RS-232 port.

Xiox XHDB - Hacker Deadbolt

The Xiox Hacker Deadbolt (XHDB) provides protection for Remote Maintenance and Testing ports of Private Branch Exchange (PBX) systems, voice-mail systems, and other Customer Premise Equipment. The XHDB can be purchased as a stand-alone unit, or as an integrated component of the Xiox Hacker Preventer. Features of the XHDB include:

Tracking Hackers Who Try to Change Systems

- Reporting on both valid and invalid attempts to access remote maintenance ports.

Stopping Hackers Who Try to Change Systems

- User configurable mixtures of spatial security, single-use with alarming, and automated connection with AI monitoring protect sensitive destinations.
- Multiple User I.D.'s and passwords for multiple users with different types of security and individual, automated profiles.
- Access protection includes up to 16 digit User I.D.'s/password combinations, and alarming.

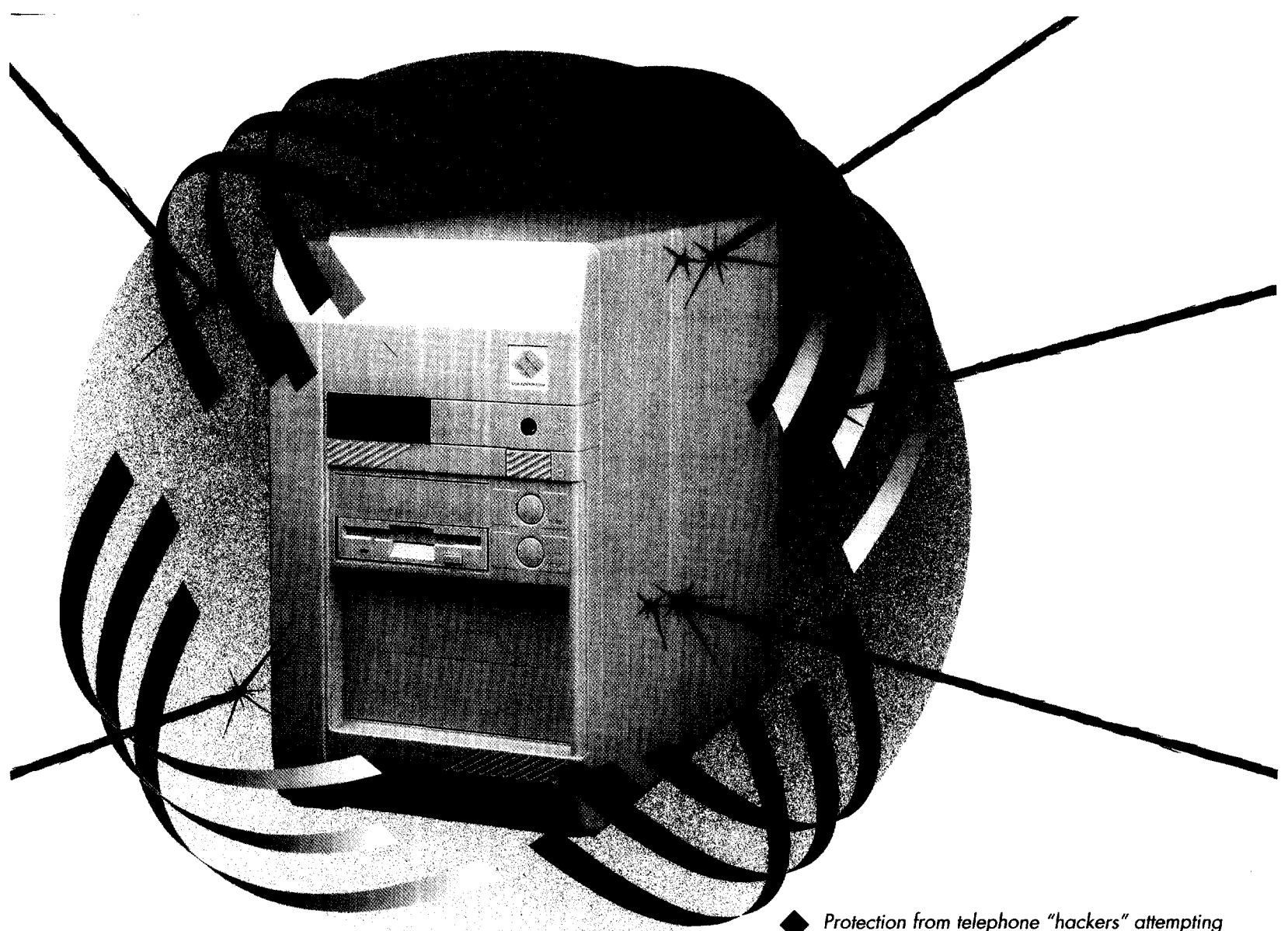
Xiox Hacker Deadbolt Technical Requirements:

- Requires 110V AC power and RJ-11 analog telephone line to XHDB unit. Requires R5232 Maintenance port connection to PBX and/or other system.



XIOX CORPORATION

• 577 Airport Blvd., Suite #700, Burlingame, CA 94010 • (415) 375-8188 • FAX (415) 342-1139
• 150 Dow St., Manchester, NH 03101 • (603) 624-4424 • FAX (603) 624-8269



- ◆ Protection from telephone "hackers" attempting to access your telecomm environment.
- ◆ Realization of remote-access service cost-savings without the risk of fraudulent use.

XHP: THE HACKER PREVENTER

The Xiox Hacker-Preventer, a member of the Xiox Fort Knox family, offers comprehensive protection against toll-fraud and other unauthorized access to your PBX and associated telecommunications equipment.

Hackers can easily attack... 800 numbers, travelling executives, telecommuters, voice-mail, automated attendants, modem pools, electronic mail, teleconferencing bridges, ACD's, telephone system networks, and remote maintenance ports. With telephone fraud in the billions of dollars annually, the XIOX Hacker Preventer is a necessary, intelligent agent for monitoring your telecomm traffic. Without penalizing your regular users, XIOX's cost-effective intelligent security targets, analyzes and prevents unauthorized access or usage of your telecommunications network!

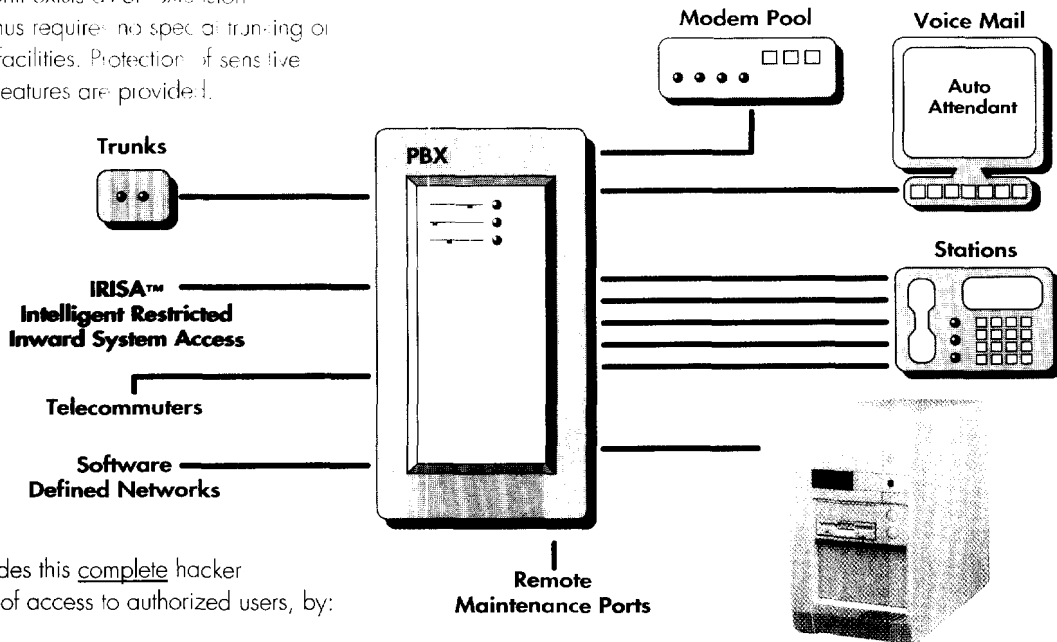
- ◆ Secure access to remote maintenance ports, voice-mail systems, and modem pools.
- ◆ Automatically and in real time senses user profile deviations and terminates fraudulent use.
- ◆ Secure monitored access for customers, traveling employees and telecommuters.
- ◆ Protection against unauthorized electronic access to vital corporate information.
- ◆ Greater visibility through printed reports on Telecomm system access.



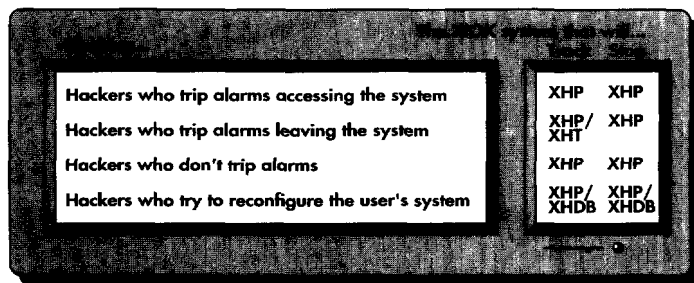
XIOX CORPORATION
Block Hacking with Force...

XHP: THE HACKER PREVENTER™ Xiox Fort Knox Family™

The Xiox Hacker Preventer is easily installed into the telecommunications network and can be fully configured and in use within hours of installation. The unit exists as an extension (or extensions) to the PBX, and thus requires no special training or installation of special telecomm facilities. Protection of sensitive destinations and remote-access features are provided.



The Xiox Hacker Preventer provides this complete hacker protection, while allowing ease of access to authorized users, by:



Tracking Hackers

- Robust reporting capabilities include Authorized User, Call Detail, Active User I.D.'s and Daily Activity by User I.D.

Stopping Inbound Hackers

- 3 levels of access protection including user I.D. and password, verbal password(s), and alarming.

Stopping Outbound Hackers

- User I.D.'s can be easily tied to specific destination or restricted from destinations, and PBX leaks are plugged automatically.

Stopping Hackers Who Don't Trip Alarms

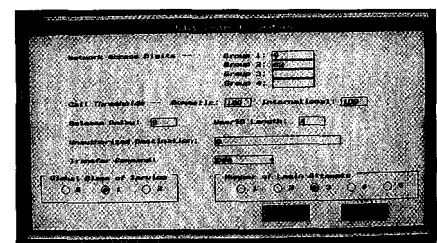
- Proprietary user profiling, automated accumulation of profiles, and artificial intelligence comparisons to profiles separates hackers from users.

Stopping Hackers Who Try to Change Systems

- User configurable mixtures of spatial security, single-use with alarming, and automated connection with AI monitoring protect sensitive destinations such as remote ports of voice-mail and PBXs.

XHP Technical Specifications

Physical	Housing: Shelf or desk mounted enclosure H 13.5 in. W 7.5 in. D 16 in. Weight, exclusive of packing materials: 28 pounds.
Electrical	Mains power: 115/230 Vac, 50 - 60 Hz, 50 VA. max, 25 VA typical
Environment	Operating temperature 10 to 50 deg. C. Relative Humidity 10 to 95%.
Telephone	RJ11 analog. FCC registration: EMC54S-15118-MDE. Req: 0.8B. UL E101818
Functional	User ID code length: 8 digits maximum, 1 digit minimum. Password length: 8 digits maximum, 1 digit minimum. Dialed number length: 28 digits maximum Global Service Classes: 0 restricted, 1 & 2 unrestricted. User Service Classes: 0 restricted, 1-9 unrestricted.
Reports	Authorized User ID list, selectable by range of user code. Call Detail Report, last in first out, 5000 call sliding window. Active User Report, selectable by range of user code. Daily Active User Report.



Configuration and maintenance can be accomplished either by telephone or using the DOS-based configuration utility provided with the XHP.



XIOX CORPORATION

• 577 Airport Blvd., Suite #700, Burlingame, CA 94010 • (415) 375-8188 • FAX (415) 342-1139
• 150 Dow St., Manchester, NH 03101 • (603) 624-4424 • FAX (603) 624-8269

CAN YOU SPOT THE COMPROMISED TELEPHONE SYSTEM?

Every telephone system can be compromised! Hackers can easily attack... 800 numbers, travelling executives, telecommuters, voice-mail, automated attendants, modem pools, electronic mail, teleconferencing bridges, ACD's, telephone system networks, and remote maintenance ports. All of these represent entry points for possible telephone fraud.

Intelligently separating hackers from legitimate callers, the XIOX Hacker Preventer™ is designed to protect your entire telecommunications network while still allowing full use of all your system's money saving features.

For more information about what telephone hackers are doing to get into your system, and how the Hacker Preventer can save your company tens of thousands of dollars, call (415) 375-8188.

"We had our
DISA shut off
and we still
lost \$75,000"

"We got hacked
through our
voice mail !?"

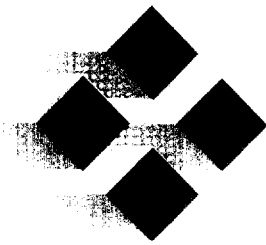
"The hackers
locked us out
of our own
system"

"We were hit
for thousands of
International calls
through
modem pools"



XIOX
CORPORATION

577 Airport Blvd, Suite #700,
Burlingame, CA 94010
(415) 375-8188



XIOX CORPORATION

**Xiox Corporation
Fort Knox™ Warranties**

Xiox Hacker Preventer Warranty is a yearly Warranty against telephone fraud financial loss caused by remote access fraud at a site protected by a XHP.

The limit of the yearly Xiox Hacker Preventer Warranty is equal to the Xiox list price or the end-user discounted price (whichever is lower) of the XHP warranted, minus a deductible per incident of \$1000 or 10% (whichever is higher).

The Xiox Hacker Preventer Warranty is underwritten by The Travelers Insurance Company.

The Xiox Hacker Preventer Warranty covers telephone fraud financial loss due to the hacker attacking and penetrating advanced features and switch adjuncts such as IRISA (tm), voice mail, modem pools, etc. The Xiox Hacker Preventer must have an opportunity to view the traffic in order for the traffic to be covered.

The Xiox Hacker Preventer Warranty covers traffic on all IXC's and LEC's. The Xiox Hacker Preventer Warranty covers both domestic and International traffic.

The Xiox Hacker Preventer Warranty for the first year cost is included in the purchase price. The second and subsequent year Warranties are available for a 4% Warranty renewal fee.

The Xiox Hacker Preventer Warranty can be applied for using an Application available from Xiox at

the time of purchase of the XHP.

Xiox Fort Knox Warranty is a yearly Warranty against telephone fraud financial loss caused by remote access fraud for single or multiple site customers with at least one XHP, and all other sites protected with a minimal Fort Knox product configuration.

The minimum Fort Knox product configuration is either a Xiox Hacker Deadbolt and Xiox Hacker Tracker, or XHDB and standalone GBS+, or XHDB and a GBS+ pollable buffer. The XHP equipped site(s) is required to have either XHT, GBS+, or a GBS+ pollable buffer.

The limit of the yearly Xiox Fort Knox Warranty is \$100,000 per customer, in aggregate, across all customer sites; minus a deductible of \$10,000.

The Xiox Fort Knox Warranty is underwritten by The Travelers Insurance Company.

The Xiox Fort Knox Warranty covers telephone fraud financial loss due to the hacker attacking and penetrating advanced features and switch adjuncts such as IRISA™, voice mail, modem pools, etc. at (the) site(s) protected by XHP(s). The Xiox Hacker Preventer(s) must have an opportunity to view the traffic in order for the traffic to be covered.

Sites with the minimal configurations of Fort Knox product are warranted not to be hacked through the maintenance ports, basic features, or latent

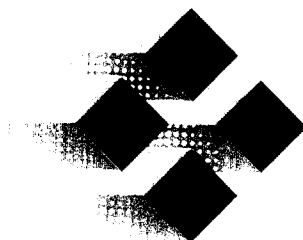
advanced features. If a site has advanced features and switch adjuncts, it will need to have a XHP in order to be included in the Xiox Fort Knox Warranty.

The Xiox Fort Knox Warranty covers traffic on all IXC's and LEC's. The Xiox Fort Knox Warranty covers both domestic and International traffic.

The cost of the Xiox Fort Knox Warranty is \$4,000 per year. This cost is the same no matter the number of XHP equipped sites vs. minimal configuration sites. The cost is the same with single or multiple sites.

The Xiox Fort Knox Warranty requires up front and yearly system audits. These audits are available from Xiox for \$1,200. System audits done by others may be accepted by Xiox.

The Xiox Fort Knox Warranty can be applied for using an Application available from Xiox.



XIOX CORPORATION

Fact Sheet

- Founded:** Founded in 1982, Xiox became a publicly held company with a successful offering of common stock in February 1986 and is traded under the symbol "XIOX" on the NASDAQ exchange.
- Market:** Xiox designs, manufactures, distributes and supports a wide range of telecommunications management systems which operate on local area networks and MS-DOS compatible personal computers. These systems can meet the simple needs of a 25 person office or the complex needs of a multi-site Fortune 500 corporation. Xiox products assist an organization in controlling telephone expenses and facilities and can also be used to improve employee productivity.
- Strategy:** Xiox targets three related markets for telecommunications management systems: The company is a leader in applying local area network (LAN) technology to replace mainframe- and mini-computer-based applications for distributed telecomm processing and reporting. The company also maintains leadership in wide area distributed processing and reporting products. Thirdly, Xiox targets telecomm system security needs by allowing telecomm system access to be managed both openly and securely.
- Distribution:** Xiox markets its systems through a direct sales force, dealers, subsidiaries of the Regional Bell Operating Companies (RBOC's) and Original Equipment Manufacturers (OEMs). The company and its dealers have sold and installed over 16,000 systems.
- Products:** Xiox Telecommunications Management Systems are a comprehensive group of separate PC-based software tools that manage a telecommunications system from top to bottom.
- The Xiox Call Accounting Series captures and tracks telephone usage data for accurate cost allocation by department, employee, guest or client.
 - The Xiox Traffic Engineering Series is a powerful management tool which provides for in-depth analysis of a telecommunications system by showing options for optimizing trunk performance and carrier service.
 - The Xiox Facilities Management Series provides full financial and operational control for more efficiently managed equipment inventory, service orders, trouble reports, cable records, cost allocation and directory listings.
 - The Xiox Fort Knox Series. Systems protected from unauthorized access with this series are secure yet open, allowing legitimate users full use of the money-saving features of their telecommunications and information systems.

Management:

William H. Welling, *CEO and Chairman of the Board*

Managing partner of Venture Growth Associates
Formerly, President of Marshall Industries
Executive Vice President of Marshall Industries
Vice President of Shuman Agnew

Michael O'Connell, *Vice President of Marketing*

Formerly, Regional Vice President, Phoenix Telecom
Vice President of Sales, Product Marketing and Market Development, Telwatch
Director of Marketing, DAVID Systems

Benjamin F. Slick, *Vice President of Sales*

Formerly, Manager, Pacific West Sales District, BT Tymnet
Account Executive, Michigan Bell Telephone

Richard J. Filak, *CFO and Vice President of Finance*

Formerly, CFO/Director of Finance of Novacor Medical Corporation
Finance, Hewlett-Packard
Finance, Spectra-Physics
Financial Consultant, Arthur Anderson & Company

David Schlossman, *Vice President of Engineering*

Chief Engineer, Xiox
Senior Software Engineer, Xiox
Software Engineer, Columbia and New York Universities

Tony DiIulio, *Vice President of Operations*

Formerly, Director of Summa Four Business Products, Inc.

Location: Headquarters 577 Airport Blvd, Suite 700, Burlingame, CA 94010. Also 150 Dow St., Manchester, NH, 03101.

NOTE TO EDITORS, REPORTERS AND ANALYSTS: These persons are available to comment on the company and its products and on market, industry and technology issues. Feel free to call the company directly or Oak Ridge Public Relations (408) 253-5042 to arrange contact with the appropriate individual.



XIOX CORPORATION

Overview

The Xiox Fort Knox Deadbolt™ (XHDB) provides protection for sensitive destinations, such as the remote programming port of the PBX, voice mail, etc.; and PC, LAN, mini-computer, and mainframe communication ports. XHDB replaces conventional, and/or existing modems with 9 user selectable, configurable security options.

The XHDB is available as a standalone device, or it can be integrated as an option in the Xiox Hacker Preventer™ (XHP). The XHDB is available in four configurations:

- Option D1- a single RS232 port
- Option D2- 2 RS232 ports
- Option D3- a single RS232 port,
with asking for
permission and pager
features; COSs B, C,
H, and I.
- Option D4- 2 RS232 ports,
with asking for
permission and pager
features; COSs B, C,
H, and I.

System Parameters

User ID and Password

Both may be configured from 1 to 8 digits, for a maximum of 16 digits, depending on security vs. ease of use trade-offs. The default value is 8 digits.

User IDs may not be duplicated, although passwords, and dial back numbers may be duplicated.

Number of Log In Attempts

Upon reaching the Deadbolt, the caller is asked for his user ID, and password. If either number

is incorrectly entered, the user will be prompted for re-entry 0-4 times, depending on user configuration. The default value is 8 digits.

Time of Day Routing

XHDB Classes of Service (COSs) A, B, and E depend on time of day settings associated with the unauthorized caller destination. The settings will define the "business hours" or day and night periods.

Dial back Number

XHDB COSs D and J require the entry of dial back numbers. The numbers may be internal or external to the PBX.

Dial back numbers may only be assigned by the system administrator. After correctly entering the user ID and password, a COS D or J user will hang-up, and be called by the XHDB, prior to connecting to the maintenance port or other sensitive destination.

A COS H user is issued a second, random password via the pager identified in the "dial back number" field.

Destination Number

XHDB COSs B, C, and I require the entry of destination numbers. The numbers may be internal or external to the PBX. Destination numbers may only be assigned by the system administrator.

After correctly entering the user ID and password, a COS B or C user will wait until the system administrator called by the XHDB gives permission to connect to the maintenance port or other sensitive destination.

XHDB COS I is intended for AT&T INADS personnel and automated systems who will not be required to enter XHDB user IDs and passwords. When COS I is used, upon answering, the XHDB outputs the destination number, connecting the COS I to the maintenance port or other sensitive destination.

Upon answering, the XHDB with COS I calls the dial back number 2 times for every access. The first dial back call to the user's pager is a notification of an attempt to reach the maintenance port or other sensitive destination. The second call to the user's pager is notification of either correct or incorrect maintenance port or other sensitive destination user IDs and passwords.

Commands

XHDB COSs E and F provide for a restriction of command codes which can be passed to the protected port. The "permitted verbs" or commands which are allowed are specified in this screen.

In addition to 5 permitted command strings, an attention or log-on string and a log-off string may be specified.

Ports

XHDB Options D2 and D4 can protect 2 RS232 ports. When these options are used there is special consideration that needs to be given to destination. If a 0 is entered in the destination field, when the user properly logs onto the XHDB, they will be asked which protected port they wish to address. If a 1 or 2 is entered in the destination field, the user will be connected to that port.

Users

Up to 9,999 user IDs with any of the 9 Classes of Service can be entered. With the exception of COS I, complete flexibility is allowed in the mixture of the COSs. If COS I is selected, only COS I may be used.

Reports

A series of reports can be requested by the system administrator. A report can be requested which lists all existing authorized users. The Authorized User Report includes a display of historical statistics relating to the activity of the specific user.

A second report can be requested which shows the details for each call processed by the XHDB, the date and time the call was received, and the disposition of the call. The report is issued on last-in-first-out so that the most recent activity can be displayed first. The system administrator can, at a glance, see if failed attempts are being made to gain access.

Classes of Service

A- Business hours only. No command code restrictions.

B- Business hours only. Permission to connect required after business hours. No command code restrictions.

C- Permission to connect required. No command code restrictions.

D- Dial back. Spatial security. No command code restrictions.

E- Business hours only. Command code restrictions.

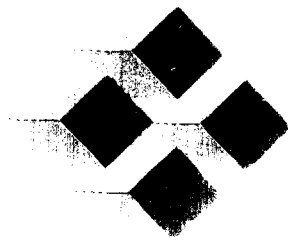
F- Command code restrictions.

G- Artificial intelligence profiling and real-time analysis. No command code restrictions.

H- Pager verification. Session specific, 2nd passwords sent to user's pager or cellular phone. No command code restrictions.

I- Code forwarding and pager notification of attempt, and correct or incorrect user ID/password. No command code restrictions.

J- System Administrator code. Spatial security. No command code restrictions.



XIOX CORPORATION

BACKGROUND ARTICLE
ON
TOLL-FRAUD PREVENTION

By:
Michael O'Connell
Vice-President, Marketing
Xiox Corporation

SEARCHING FOR COMPLETE TOLL FRAUD PROTECTION

It seems every day we hear about another company hit by hackers, and almost everyday we read about another toll fraud product unveiled as the latest panacea. "Solutions" range from the simplistic suggestion of unplugging DISA, Direct Inward System Access, to sophisticated hardware and software tools. Each solution, however, addresses only a part of the problem: minimally secure DISA lines, vulnerable maintenance ports, or hackable voice mail systems. Before we rush to embrace a particular solution in hopes of a sense of security, we need to take a few steps back and take in the entire scope of the problem. Only then can we put together the best protection for our telecom systems.

Protecting our telecommunications systems is in many ways analogous to protecting our homes. Just as we would never drive away from our house with all the doors and windows open, and all our valuables sitting on the kitchen table, neither should we leave our telecom system unprotected and vulnerable to amateur and professional hackers.

The worst thing that could happen to a home owner is for the burglar to get a hold of the keys to the house. The burglar could enter now; or at any time in the future, sneaking in and causing damage over and over again. Or, once the burglar was inside the house they could lock the homeowner out of the house. When a hacker obtains the remote access passwords they become the burglar with keys.

Consider the risk; there are numerous ways hackers can break into most telecom systems. Once in, hackers resell the means of entry to other hackers, who in turn can fill your trunks with their traffic, leaving long distance bills of tens or

hundreds of thousands of dollars in their wake. We have all heard the stories. The risk is real. If you haven't been hacked yet, you probably think it can't happen to you. You're wrong, it can. And if you have been hacked, you know it could happen again.

How then do we best protect all our equipment: our PBX, voice mail, automated attendant, DISA, remote access ports, modem pools, and tandem connections to SDN?

Going back to the analogy of protecting a house, the first step is to install locks on the doors and windows - using some form of password protection. There are a number of companies offering password protection products. Some use long numbers, which are difficult to crack. Others use voice prints. Some use cards with ever-changing password numbers.

Password protection is certainly important, but it is not enough. Passwords need to be non-sequential, preferably 8 or more digits, and absolutely not the system's default password. Even though they provide a good first level of protection, passwords can be compromised: passcards can be lost, passwords can be observed or videotaped in public places, and hackers using computerized speed dialers can break an 8 digit code in a matter of hours.

In response to better and better hacker tools called "War Dialers," some companies are looking at longer than 8 digit passwords. Now the user is being penalized by more digits to remember and dial, and the hacker's response is just to get better tools.

Voice identification combined with passwords provides additional security, but also has drawbacks. While these systems effectively prevent computerized dialers

from gaining direct access to the system, if the voice match requirements are too tight, legitimate users may be locked out of the system due to background noise, or a change in the users voice, such as if the user has a cold. If the voice match is too loose, the password can be overheard and used by hackers. If the phone booth is bugged in order to get the digits dialed by running the tape through a PC program, the hackers can play the tape of the voice identification over and over again from multiple places all over the city.

These solutions are the equivalent of putting bolts on the doors and locks on the windows. Unfortunately, as fast as companies develop new locks, hackers are developing new lock picks. Locks are important, but not enough.

Many users have also taken the action of boarding up some of the doors and windows. By shutting off their DISA lines, shutting off the Voice Mail feature, and unplugging the remote access ports, they have "gone dark" in hacker parlance.

The disadvantage of going dark is boarding up the house keeps the owner of the house on the outside too. Users who go dark then lose the significant savings that features such as DISA provided. The DISA savings of up to 40% over credit cards helped cost justify the PBX purchase.

What is needed beyond locks on the door is a 24 hour per day, 7 day per week Private Security Guard that lets users in with a friendly nod, keeps the hackers out, and immediately sets off alarms when hackers try to break-in. Or instead of the real live guard, artificial intelligence that can act just like the guard. Such an Intelligent Restriction on Inward System Access (IRISA) would provide the DISA savings, without the DISA drawbacks.

After securing the doors and windows, the next step is to limit the valuables that can be taken if someone does get inside your house. Just as you shouldn't leave your valuables in a place accessible to anyone, you need to restrict the amount of theft a

hacker can commit. The valuables should be stored in a hidden home safe.

Carrier plans that insure only their own traffic are analogous to placing only some of your valuables in a safe, and not protecting the others. Also, the carrier versions of safes only work when all the doors and windows are boarded shut. The carrier insurance plans requirements on systems would keep out legitimate users along with most hackers.

This hidden home safe needs to limit the type and amount of calls that could be made once entry is achieved. This would require being able to distinguish between the legitimate user's calls, and those of a hacker.

The system needs to know what legitimate user's calling patterns look like. And it needs to be able to monitor each call against what is a normal calling patterns for that user. If the system detects a call that varies from the users normal pattern, outside of predetermined limits, it should be able to notify the System Administrator. If the system is unable to reach the System Administrator, it should be able to take protective action on its own.

Protective actions need to be taken, such as tightening up all the security features - strengthening the locks, shrinking the size of the doors and windows, and sealing the home safe until help can arrive. In telephony terms this might be starting to ask for voice matching along with the password, allowing fewer user mistakes before disconnecting, and rerouting certain calls to the Telecommunications Security Department.

Maintenance ports are the keys to the kingdom for the hacker. Having a hacker get into your system's maintenance port is like losing your keys to a dishonest locksmith. Hackers enter maintenance ports to turn DISA back on when it's been shut off, turn on voice mail outdial features, shut off call accounting overnight in order to hide their trail, and create phantom extensions with 3-way calling to use for

hacking. Hackers can even lock the system administrator and their service provider out of the system.

In order to keep from losing the keys to a dishonest locksmith, some companies have developed security products, using combinations of locks and keys that only allow one copy of the key. Other products operate by dialing back to one location. The disadvantages to these systems are interference with the normal method of switch maintenance and the need to protect other systems beyond the PBX.

The switch maintenance provider that has the traveling technician, their foreman, and/or the maintenance center(s) ready to respond to a switch alarm is providing the best options for service. A single key or dialback to only one location will limit the service provided by the maintenance provider.

Not only do hackers attack the switch maintenance port, they also attack the maintenance ports of voice mail, automated attendants, and teleconferencing bridges; as well as the ports of modem pools, and electronic mail systems.

What is needed to protect all the keys to the system is a flexible, user definable combination of alternatives that intelligently balance the ability to provide the highest degree of maintenance to all systems and the need to be protected. Alternatives should include multiple dialback locations, passwords that are only allowed to be used for the day, and passwords that are only used once and automatically cause an alert call to the owner of the system. With all of the alternatives, the artificial intelligence that acts like a private security guard should watch the use of the passwords.

Call accounting systems can be used like the surveillance cameras protecting the house. Properly used, the call accounting system can help the system owner to identify hacking attempts, or detect new methods of hacking being tried out before the weekend of tens of thousands of hacking calls, and share information with

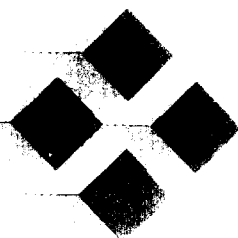
other system owners - good guys, and hopefully prosecute the bad guys.

Just as a surveillance camera cannot film the side of the house that is out-of-sight, call accounting cannot track the bad guys if it cannot see or recognize the hacking call records. Hackers know how to damage the call accounting record to stop the average call accounting system. Within the industry, a number of the call accounting systems have the ability to see and report on the damaged call record.

As a method of summing up what is needed in a complete toll fraud product, the following matrix should be filled out by the system or systems used both on the customer premises and available through the carriers network(s):

	Track	Stop
Hackers who trip alarms accessing the system	X	X
Hackers who trip alarms leaving the systems	X	X
Hackers who don't trip alarms	X	X
Hackers who try to reconfigure the users system	X	X

If the matrix is not completely filled in, we are vulnerable to a hacker attack. Some of the elements are harder than others to fill in. Tracking and stopping the hackers that don't trip alarms, the bad guys that disguise themselves as good guys, is probably the hardest. However, with the cost of not stopping and tracking all types of hackers potentially being in the millions, the effort is worth the cost.



XIOX CORPORATION

NETWORK

SECURITY

ASSESSMENT

**CALL-ACCOUNTING
SAMPLE REPORTS**

** These reports were generated using Xiox General Business Software™ Version 4.0.*

*For more information on how Xiox call-accounting can help you secure your system,
please contact Xiox Corporation at (415)-375-8188.*

INTRODUCTION

The following call-accounting reports are representative of those that should be generated and examined using a fully-featured call-accounting system such as the Xiox General Business Series™. In general, users wishing to monitor their system for potentially fraudulent activity should watch for a number of warning signs:

Early Stages:

- An increase in inbound 800 traffic, particularly on remote access facilities such as DISA
- Large number of uncompleted calls or calls of short duration
- Increased outbound 950, 900, and 700 traffic
- Higher than normal odd-hour usage
- Increase in reported "obscene" or "strange" calls to personnel, especially those at points of system access such as operator or receptionist.
- Calls appearing to originate from unknown extensions or trunks

Later Stages:

- Drastic increase in international and domestic long-distance traffic
- Steady, and heavy, traffic at odd-hours
- Increased blockage of inbound remote access facilities
- Numerous calls to 809 area code and to countries in South America, the Middle East, and Europe (common destinations of hacked traffic).

These are just a few of the signs that might indicate that telephone hackers are trying to gain access to your system.

Using Xiox call-accounting, all of these signs can be detected *before* serious abuse occurs. By running reports on specific area codes, country codes, or NXX's (such as 950) potentially fraudulent traffic can be detected and dialing access can be restricted.

Xiox call-accounting can also help uncover a hacker's attempts to dial out on your system by capturing call-detail for uncompleted calls. Many call-accounting systems discard call-detail records with unrecognized dialing patterns, which can be up to 33% of all records. Xiox call-accounting systems retain all records delivered by the PBX, even if the dialing pattern is unrecognized. This allows the user to examine call-accounting reports for calls from "phantom" extensions--often extensions created by hackers--and for trunk to trunk calls identified by a trunk number appearing in the extension field.

While the reports on the following pages are representative of those that are often used to detect fraudulent activity, a Xiox system can produce many more reports than those included. Additionally, using call-accounting is just one of the many steps user's can take to prevent fraudulent traffic. Contact your local Xiox representative to learn more about protecting yourself from hackers. *We're here to help!*